TABLE OF CONTENTS

CERTIFICATE OF MAILING/TRANSMISSION (37 C.F.R. 1.8A)

I hereby certify that this correspondence is, on the date shown below, being:

MAILING

✓ deposited with the United States Postal Service, with sufficient postage, as first class mail in an envelope addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

FACSIMILE

_____ transmitted by facsimile to the Patent and Trademark Office.

Lisa L Pringle

Signature

Date: 6/16/05

Lisa L. Pringle

(type or print name of person certifying)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re application of:

Kenneth W. Aull

Serial No.: 10/027,622

Filed: December 19, 2001

Group Art Unit: 2133

Examiner: Nadia Khoshnoodi

For: *Assignment of User Certificates/Private Keys In Token Enabled Public Key Infrastructure System*

DECLARATION UNDER 37 C.F.R. §1.131

Sir:

I, the undersigned, declare as follows:

1. I am an inventor of the invention entitled Assignment of User Certificates/Private Keys In Token Enabled Public Key Infrastructure System, disclosed and claimed in U.S. Patent Application Serial No. 10/027,622 (hereinafter to as "the Application"), which was filed on December 19, 2001.

2. I along with my co-inventors, Thomas C. Kerr, William Freeman and Mark A. Bellmore, conceived the subject matter that is disclosed and claimed in the Application prior to December 20, 2000, while employed for a predecessor-in-interest to the Assignee.

3. Prior to December 20, 2000, I prepared a written description in the form of a PowerPoint® presentation of various aspects of a PKI architecture, including the subject matter claimed in the Application. The written description was updated on November 9, 2000, presenting evidence that the subject matter was conceived at least prior to November 9, 2000. A copy of this written description is attached hereto as Exhibit A.

4. On January 4, 2001, I completed a second written description in the form of a PowerPoint® presentation of various aspects of a PKI architecture, including the subject matter claimed in the Application. A copy of this second written description is attached hereto as Exhibit B.

5. On February 20, 2001, I submitted an invention disclosure relating to the application. A redacted copy of the invention disclosure is attached hereto as Exhibit C.

6. On April 27, 2001, a facsimile from Lorna Schott (Patent Administrator for the Assignee) requesting preparation of a patent application was forwarded to Donald E. Stout, Esq. at the law firm of Antonelli, Terry, Stout & Kraus, LLP. The facsimile included the disclosure for the invention described in the Application under docket number 15-0257. A redacted copy of the facsimile is attached hereto as Exhibit D.

7. On Tuesday, June 25, 2001, George N. Stevens sent a letter to Lorna L. Schott that that included a draft of the Application, which was prepared by the law firm of Antonelli, Terry, Stout & Kraus, LLP. A redacted copy of the letter is attached hereto as Exhibit E.

8. After a review of the draft of the Application, on October 18, 2001, a letter including a marked up copy of the draft of the Application was sent to George N. Stevens of the

law firm Antonelli, Terry, Stout & Krous, LLP. A redacted copy of this letter is attached hereto as Exhibit F.

9. On October 24, 2001, another draft of the Application was included in a letter to Lorna Schott. A copy of this letter is attached hereto as Exhibit G.

10. I believe that the Application was filed in the U.S. Patent Office on December 19, 2000.

11. I declare that all statements made herein of our own knowledge are true and that all statements made on information and belief are believed to be true; and further that these statements were made with the knowledge that willful false statements and the like so made are punishable by fine or imprisonment, or both, under §1001 of Title 18 of the United States Code and that such willful false statements may jeopardize the validity of the application or any patent issued thereon.

Kenneth W. Aull June 16, 2005

Kenneth W. Aull Date

[redacted] Class 4 PKI
The Winning Technical Strategy

Ken Aull

11/9/2000

[redacted] Class 4 PKI
A complex Customer set (8)

TRW

☐ Many Oars are in this water

- [redacted] - Art Money
  - » Sponsor of the project - has directed that the players below be nice or lose their money
- [redacted] Class 4 Program Office
  - » Program Manager - [redacted], assigned out of [redacted]
- [redacted]
  - » [redacted] is the customer for the system. They run the Class 3 system, which by direction will be replaced with the [redacted] Class 4 system
- Common Access Card (CAC) Program
  - » Run by the [redacted], a forced marriage with the [redacted] Class 4 PKI
- Global Information Grid
  - » These people supply the Directory technology for the [redacted]
- [redacted] and the [redacted] initiative ([redacted])
  - » [redacted] will evaluate the security - They see this as funding for their [redacted] program
- 22 Independent Agencies of the [redacted] - Have the bulk of the money
- Users - Not represented by anyone but the prime integrator

What is the winning technical strategy?

TRW

☐ TRW Enterprise Directory and Security (TEDS)

- Not the solution for the [redacted] without significant modification
- [redacted] depends on Apriori Authoritative sources
- [redacted] policy defines users post facto
- [redacted] depends on a well defined management structure
  - » [redacted] Chain-of-Command not well suited to this requirement
- [redacted] assumes a reasonable level of paranoia about security
  - » Technical evaluation team defines new heights of "what if" paranoia

☐ What TRW brings is an uncommon concern with

- High Security
- Low Cost
- Strictly enforced processes and procedures
- Replaceable COTS structures
  - » Have used both Netscape and E-Certify

The Local Registration Authority (LRA)

TRW

- The LRA is the Achilles Heel of PKI
  - A Classic LRA costs 1 full head per 2000 users
- [redacted] eliminated the LRA
  - The manager became the Face-to-Face agent
- Elimination of the LRA in the [redacted] is not possible
  - The CAC officer is the LRA - a given
  - There is no authoritative source for manager
  - One of the constituents is the CAC program
    - » Will not look favorably on being eliminated
- Many of the 22 agencies ([redacted] for example)
  - Will have their own badges
  - Need to be incorporated into the process
  - These are an unfunded liability to the program

CLASS 4 Operations - an opportunity

TRW

- Class 4 implies a hardware token
- The hardware token opens the opportunity for TRW
  - Keep the CAC operators, but add no PKI overhead
  - Easily add badging operators from 22 Agencies
  - Eliminate cost of LRA function to support PKI
- The TRW primary Golden-Goo-Goo (G^3)
  - Make the CAC operator a badging operator (as intended)
  - CAC operator does no explicit LRA functions
  - User visits CAC only for badging functions
    - » To obtain the first badge
    - » To get a loaner badge for a temporary displacement
    - » To get a replacement badge for a lost badge
    - » To return a badge during check-out

The TRW CONOPS

TRW

- **TRW concept is for an "invisible" LRA**
  - **Functionality is hidden from the badging officer and user**
  - **Badging officer does standard functions**
    - » Identifies User via paper process
    - » Checks against "database" of users (e.g. Deers/Rapid for CAC)
    - » Checks for existing badge (Class 4 keeps record)
    - » Creates badge, including picture, fingerprint, and PKI certificate
    - » Allows user to create a PIN for the badge
    - » Signs the badge out to the user (Face-to-Face)
    - » Cancels any lost badge
    - » Issues temporary badges, logs and destroys returned badges
  - **From the view point of the user and the badging officer**
    - » PKI appears to add no additional complexity
    - » Common soldier is done, no further action required, ever
    - » No additional labor over issuing a plastic badge as currently done
    - » User never revisits the LRA for ANY PKI related reason
    - » No labor expended for the support of PKI

TRW CONOPS

TRW

- **Simple user visits badging office for a badge**
  - **User comes away with a badge**
    - » Picture for humans
    - » Digital Signature for computers and documents
  - **If badge is lost or expires**
    - » Returning to the badge office restores picture and Digital signature
    - » Cancels (revokes) any private key stored on token
  - **Temporary badge creates a one-day signature**
    - » Does not require canceling the permanent badge or certificate
    - » No flooding of the Certificate Revocation List (CRL)
  - **Returned badges only require physical destruction of badge**
    - » Physical destruction eliminates any chance for use
    - » Does not require flooding of the Certificate Revocation List (CRL)

TRW Conops

TRW

- **Office worker will require Encryption certificate**
  - TRW approach allows remote generation of encryption keys
  - The private key can only be unlocked on the token (G^3)
  - The identity of the User and Badge is crytologically sound (G^3)
  - The function happens on an untrusted workstation (G^3)
    - » Removes the labor of visiting the badge office
    - » Travel, badge officer time, user time are all saved
- **Recovery of Encryption certificate is the same**
  - User uses token for identification
  - User recovers directly the encryption certificate and keys (G^3)
  - Keys are never exposed to the untrusted Workstation (G^3)

TRW Conops

TRW

- **Organizations will require Role Certificates for users**
  - Roles are created by TRW E-Form Process (G^3)
  - Roles members are managed by Role Owner identified in Form (G^3)
  - Process is entirely electronic, and definable by Sponsor (G^3)
  - Greatly simplifies the day to day management of [redacted]
- **Users will require Certificates for their roles**
  - User can get own role certificates via the Web (G^3)
  - No LRA is involved, just the token, the Pin and Role (G^3)
    - » Major savings in travel, LRA time, User time
  - Existing private key is RESIGNED into a role Certificate (G^3)
  - Unique process means its safe on an untrusted workstation (G^3)

TRW Conops

TRW

- **Users will have many, many badges and certificates**
  - **A different badge is required on the [redacted] and [redacted]**
  - **Only 3.1M users will have CAC, 1M will have something else**
  - **Many users will have a CAC, one or more organizational badges**
    - » **Typical user may have four badges**
  - **By the nature of the token, each badge has multiple certificates**
    - » **Personal Identity sponsored by the badge issuer (CAC model)**
    - » **Personal Encryption certificate for primary email**
    - » **Personal Encryption certificates for secondary email addresses**
    - » **Role certificates for within the organization for signing**
    - » **Role certificates for within the organization for encryption for role**
    - » **Historical encryption certificates**
    - » **Typical badge may have from 1 to 8 certificates**

TRW Conops

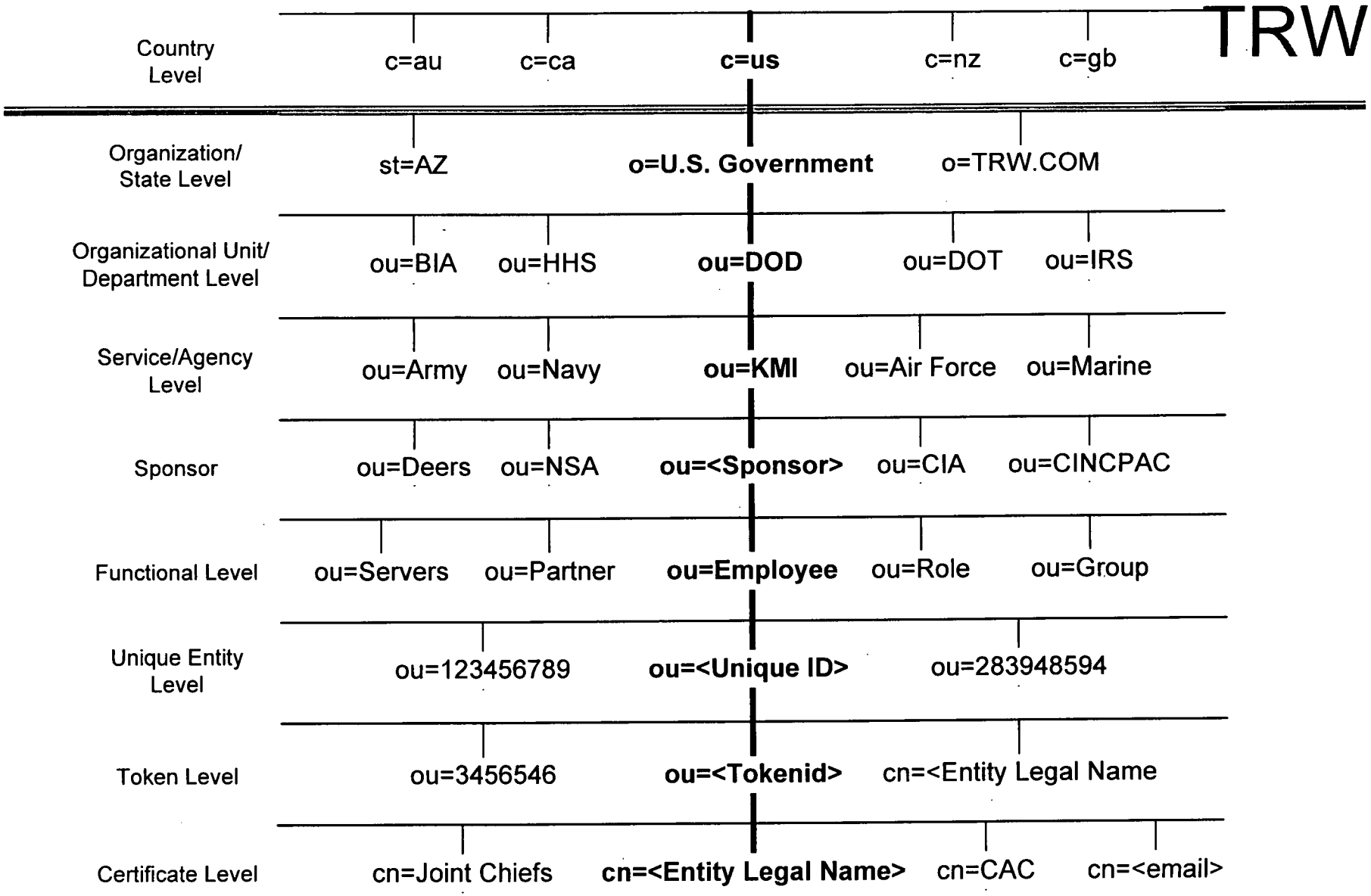
TRW

☐ TRW structures the [redacted] directory for GIG/PKI

- Directory is substructured by sponsor (G^3)
  - » Recognizes a person can have many sponsors (CAC, 22 agencies)
- Directory is substructured by type of sponsored entity (G^3)
  - » Employees, partners, customers, Servers, Roles, Groups
- Directory is substructured by Entity Identity (G^3)
  - » Each Sponsor supplies unique World Wide ID (WWID)
  - » Prevents identity theft
- Directory is substructured by Token (G^3)
  - » Recognizes multiple badges per identity
  - » Provides for temporary badges, prevents badge theft
  - » Provides for multiple classification levels ([redacted])
- Directory is substructured by Certificate (G^3)
  - » Recognizes many certificates/keys per token
  - » Allows autorevoke of lost token

☐ TRW approaches uses replication for GIG (G^3)

TRW


Country Level
c=au
c=ca
c=us
c=nz
c=gb
Organization/ State Level
st=AZ
o=U.S. Government
o=TRW.COM
Organizational Unit/ Department Level
ou=BIA
ou=HHS
ou=DOD
ou=DOT
ou=IRS
Service/Agency Level
ou=Army
ou=Navy
ou=KMI
ou=Air Force
ou=Marine
Sponsor
ou=Deers
ou=NSA
ou=<Sponsor>
ou=CIA
ou=CINCPAC
Functional Level
ou=Servers
ou=Partner
ou=Employee
ou=Role
ou=Group
Unique Entity Level
ou=123456789
ou=<Unique ID>
ou=283948594
Token Level
ou=3456546
ou=<Tokenid>
cn=<Entity Legal Name
Certificate Level
cn=Joint Chiefs
cn=<Entity Legal Name>
cn=CAC
cn=<email>

The G^3 Summary - User

TRW

☐ From the User Viewpoint - Its just a badge

- Soldier - a badge is issued with a PIN
  - » Used to sign things and visit web pages - that's all that is needed
  - » Never visit the badge office unless the badge expires or is lost
- Office Worker - a badge is issued with a PIN
  - » Used to sign things and visit web pages
  - » Also used to encrypt files and emails - self handled
  - » Recovery of historical files - self handled
  - » Never visit the badge office unless the badge expires or is lost
- Organizational Worker - a badge is issued with a PIN
  - » Used to sign things and visit web pages
  - » Also used to encrypt files and emails - self handled
  - » Recovery of historical files - self handled
  - » Issuance and recovery of role keys - self handled
  - » Never visit the badge office unless the badge expires or is lost

☐ Replace the badge every 3 years, its easy

The G^3 Summary - 22 Agencies

TRW

- Each Agency controls its badging system
  - Identity totally under the control of the sponsor
    - » Identity certificates automatically issued
  - Badging under the control of the sponsor
  - PKI entities under the control of the sponsor
    - » Employees, Partners, Customers, Servers, Roles, Groups
  - Agency issues their own tokens
  - No additional operational costs at the badging office
  - Automated E-Forms system for creation of PKI entities
    - » Easily tailored to Agency requirements
  - Encryption and Role certificates - Self Handled
- Full Control of their entities
- Minimum Cost to maintain full security
- Minimal disruption and training

The G³ Summary - [redacted] and [redacted]

TRW

- The [redacted] - a high security underpinning for [redacted]
  - Primary identity key-pair generated at a trusted workstation
  - Private identity key is generated on the token itself, never leaves
  - Happens invisibly during badge generation
  - Full Face-to-Face and ink signature collected as part of badging
  - Additional identities, such as roles, are resigns of private key
    - » This can be done safely on untrusted workstations
    - » A major advantage for the next generation [redacted]
  - Encryption certificates are generated at the central facility
    - » FIPS-140-3 level key generates assure the highest quality keys
    - » Keys are returned wrapped in the public key of the owner
    - » Can only be recovered on a specific token, by a specific user
    - » Fully secured even on an untrusted workstation
    - » Key recovery mechanism is fully automated for self recovery
- High Security and Low Cost, a win for [redacted]

TRW

Improving Key Generation & Delivery Processes for [redacted] Smart Cards

04 January 2001

Our PKI Background – Pilots (2) TRW

TRW Pilot Sep 99 – Jan 01 Netscape CMS CDC X.500 Directory fed by TRW HR's PeopleSoft database	• 1000+ X.509 signing certificates issued to employees, servers, roles, customers • VPN using Aventail servers • Employees authenticate from home using Aventail clients
JNJ Pilot Apr 00 – Jan 01 E-Certify RA/CA Isode X.500 Directory	• 200+ signing certificates for employees, servers • Signatures for HTML based forms •7 separate pilots for PK enabled applications

Production PKI Rollout Plans

TRW

TRW Feb '01 launch Encapsulated E-Certify RA/CA CDC X.500 Directory fed by TRW HR's PeopleSoft database	• 130,000 X.509 dual certificates being issued to employees, servers, roles, partners • VPN using Aventail servers • Digitally signed JettForms (XML) • ~Class 2, 3, & 4 certificates
[redacted] Feb '01 launch Encapsulated E-Certify RA/CA Microsoft Active Directory	• 190,000 dual certificates to be issued to employees, servers, roles, partners, customers • Digitally signed JettForms + proprietary HTML based forms •Class 4 only

Recent Insights, Lessons Learned TRW

- If tokens have a digital identity, great things are possible
  - Discrimination between Class 2, 3, 4 certificate stores
  - Recognition of TRW versus non-TRW tokens
  - Secure, high integrity data path from CMS all the way to the token over any non-secure network, through un-trusted workstation
- Greatest long term cost savings will come from transition to signed XML forms, automated workflows
  - Eliminate most paper forms and people to push them
  - First example is reduction of labor for PKI O&M
- Tighter security, accountability, auditability
  - Non-repudiation if forms and data signed digitally
  - Data integrity if forms serialized, auto-filled, and signed by CMS

IR&D Design Goals

TRW

- Improve speed, security, & data integrity of key generation and key distribution
- Reduce number of potential points of failure
- Reduce complexity of LRA workload
- Reduce overall life cycle cost
- Eliminate need for trusted LRA workstations
- Eliminate need for personnel to re-visit LRA to obtain additional certificates (roles, encryption…)
- Simplify processes for historical recovery of encryption certificates

Rationale

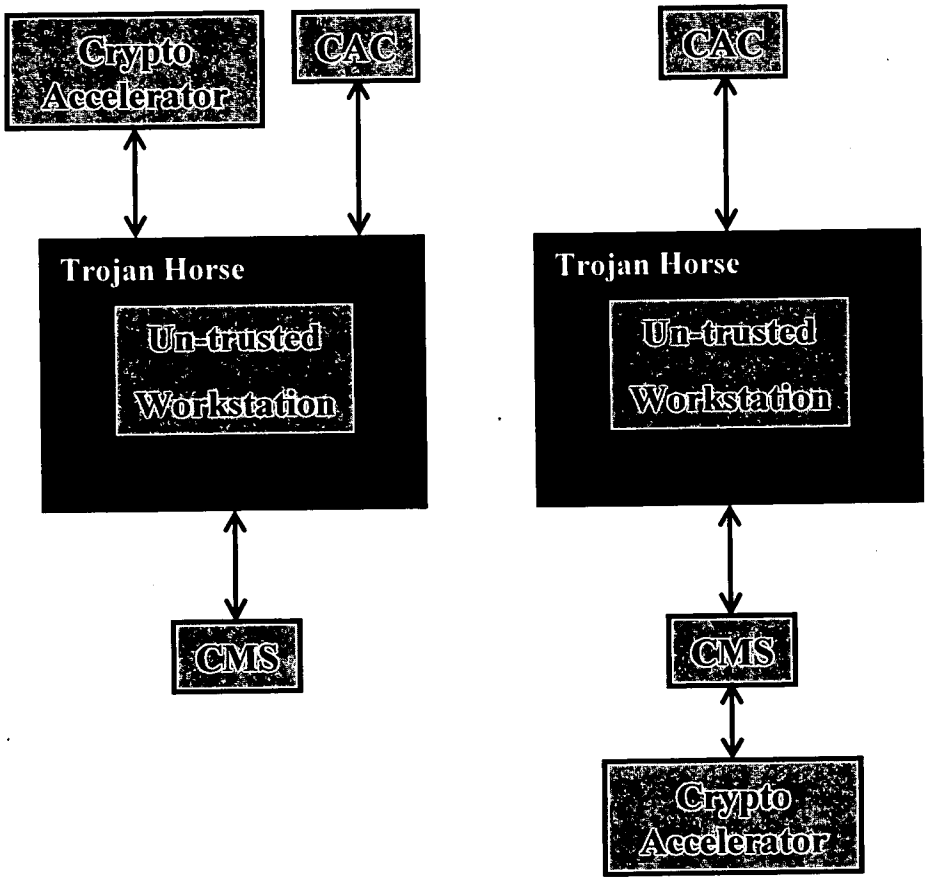
TRW

- Need for trusted LRA workstations driven by need for trusted communications between workstation & Smart Card
- Potentially simple solution:
  - Validate existing standards-based way to give each Smart Card a private key for unwrapping encrypted private keys & certificates
  - Have CA retain each card's corresponding public key in protected database or directory branch
  - Have CA wrap (encrypt) and sign all certificates intended for storage on a Smart Card using that card's public key
  - Requires only 2 trusted Smart Card key generation systems world-wide

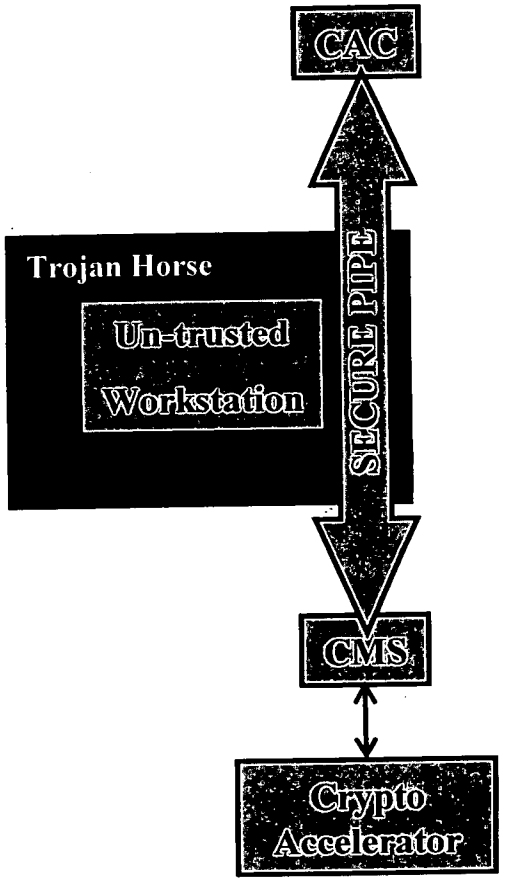
Potential Problem & Solution

TRW

Potential Problems:

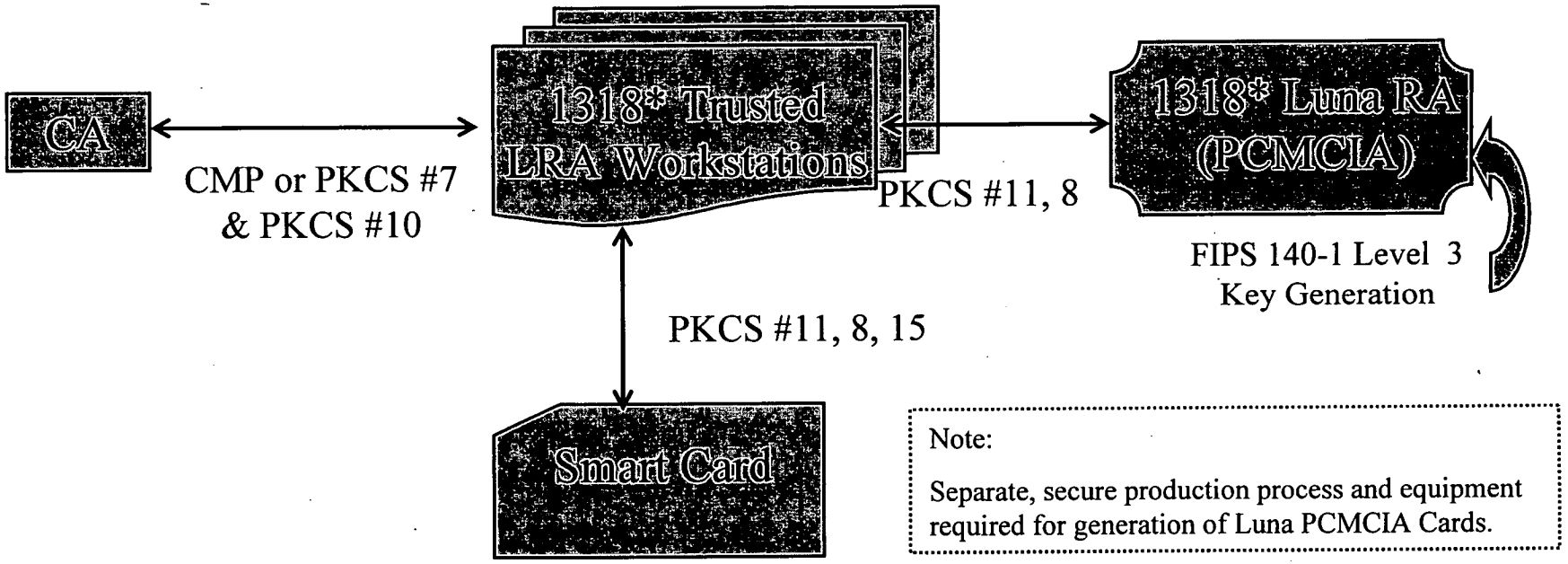


Needed Solution:



Technical Approach #1

TRW



Note:

Separate, secure production process and equipment required for generation of Luna PCMCIA Cards.

[redacted]

Pros/Con for Approach #1

TRW

- ✓ Faster, more robust key generation
- ➢ Sample costs for RAPIDS based CAC
  - o 1318 trusted workstations/environments for LRAs
  - o 1318 Chrysalis Luna PCMCIA Cards (~ $28M)
  - o Processes/facility for Luna PCMCIA Card generation
- ➢ LRA is still a critical PKI component and weakest security link (1318 potential points of compromise)
  - o Higher skills required than shown by current Class 3 PKI's E-1s and foreign nationals
- ➢ "Non-repudiation" of private key could face legal challenge since not generated on Smart Card

PKCS #12, Section 3.1, Exchange modes

TRW

There are four combinations of *privacy modes* and *integrity modes*. The privacy modes use encryption to protect personal information from exposure, and the integrity modes protect personal information from tampering. Without protection from tampering, an adversary could conceivably substitute invalid information for the user's personal information without the user being aware of the substitution.

The following are the privacy modes:

- ***Public-key privacy mode:*** **Personal information is enveloped on the source platform using a trusted encryption public key of a known destination platform (see Section 3.3). The envelope is opened with the corresponding private key.**
- ***Password privacy mode:*** Personal information is encrypted with a symmetric key derived from a user name and a privacy password, as in [15]. If password integrity mode is used as well, the privacy password and the integrity password may or may not be the same.

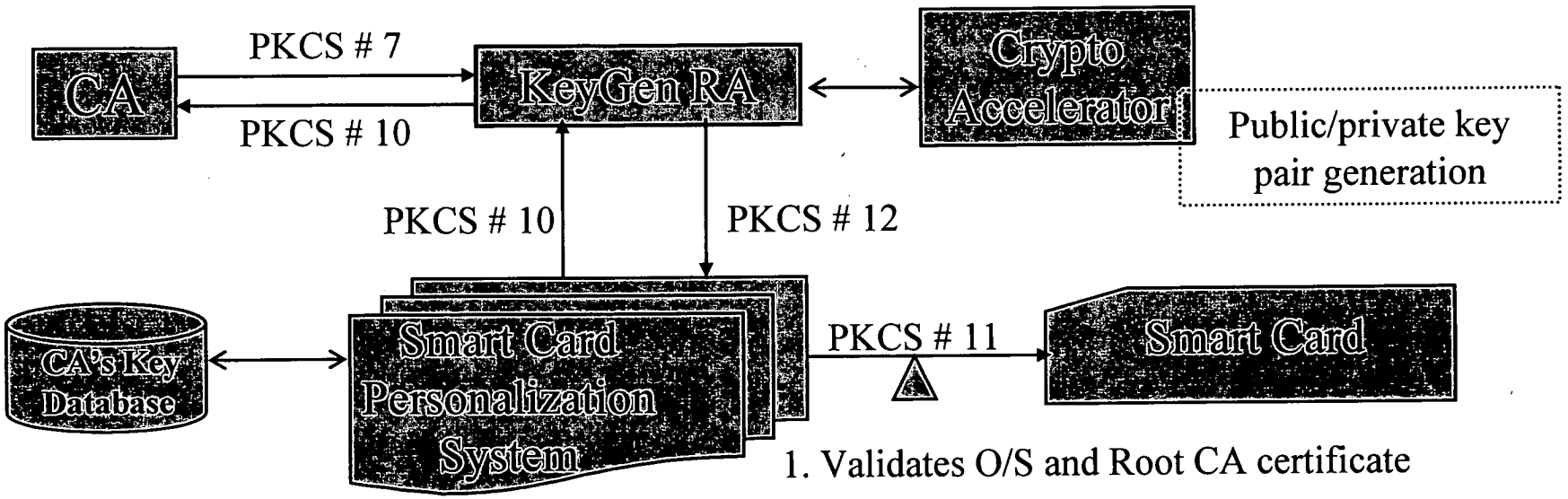
The following are the integrity modes:

- ***Public-key integrity mode*****: Integrity is guaranteed through a digital signature on the contents of the PFX PDU, which is produced using the source platform's private signature key. The signature is verified on the destination platform by using the corresponding public key (see Section 3.4).**

  Password integrity mode: Integrity is guaranteed through a *message authentication code* (MAC) derived from a secret integrity password. If password privacy mode is used as well, the privacy password and the integrity password may or may not be the same.

Technical Approach #2

TRW



1. Validates O/S and Root CA certificate
2. Writes card's Private Key to S.C. ROM
3. Writes card's key encipherment certificate to protected database or directory branch

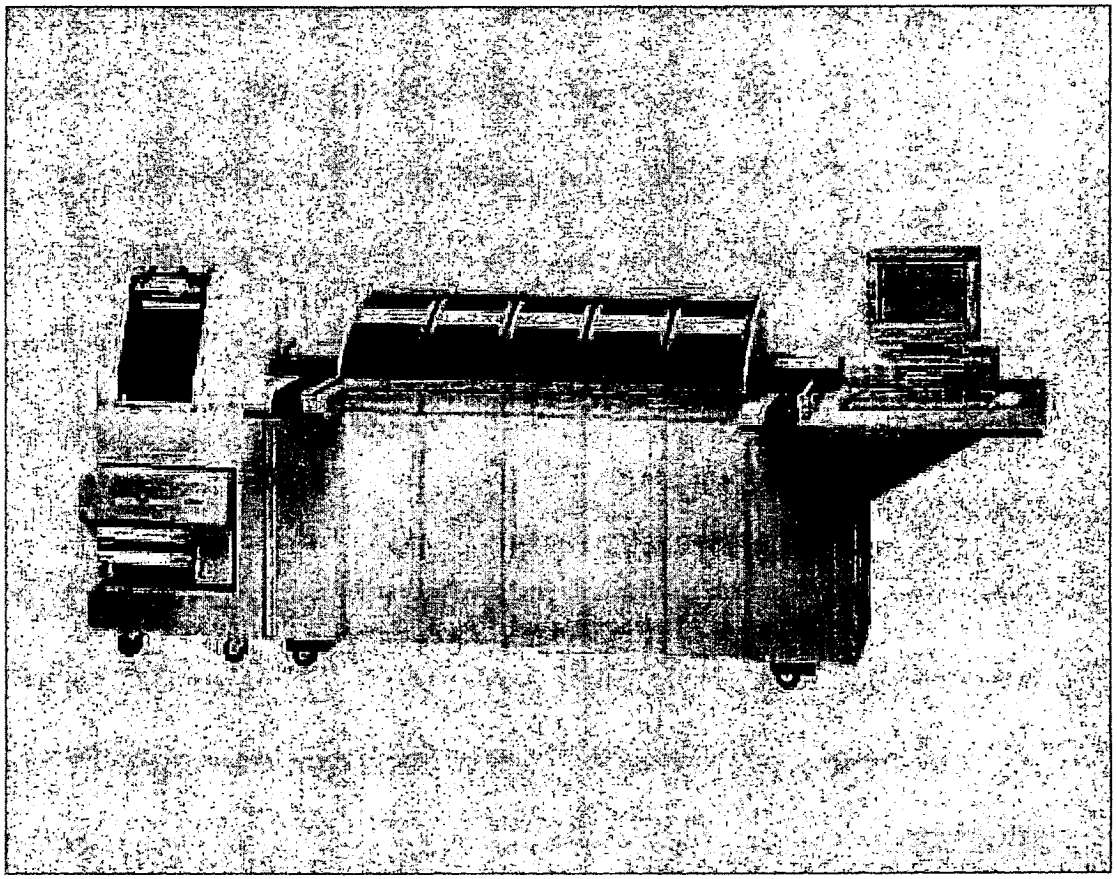
Technical Points - Approach #2 TRW

- PKI Smart-Card Key Generation System (S-CKGS) would be installed in PKI containment facilities
- S-CKGS validates O/S load and Root CA certificate for Smart Card
- S-CKGS generates unique 1024 bit key pair for each serialized Smart-Card using FIPS 140-1 Level 3 crypto accelerator
- CA signs card's public key into Key Encipherment certificate with OU=<Smart Card serial number>
- Smart Card's certificate (public key) written to protected PKI database (only CA has access to public keys for Smart Cards)
- S-CKGS writes card's private key to Smart Card ROM

➢ ***DataCard 9000 can perform this process at 900 cards per hour***

DataCard 9000

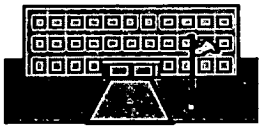
TRW



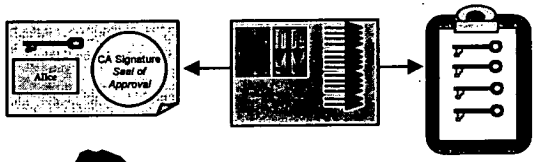
CONOPS for Smart Card Based PKI

TRW

1. Smart cards are drop-shipped to CMS facility

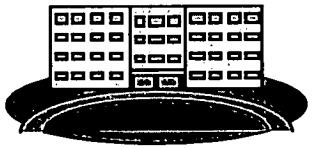


2. Smart cards are loaded with unique key wrapping keys



3. Secret key for each smart card is saved

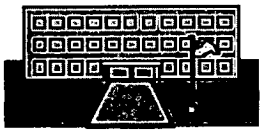
4. Smart cards shipped to badging facilities



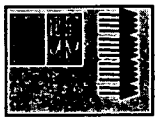
5. User visits badging Facility, presents credentials

6. Badging Officer reviews credentials

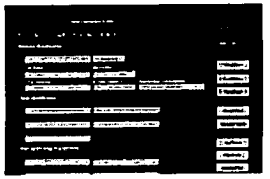
7. Badging Officer signs request for E-form with user id, Smart card ID, & organization code



8. CMS checks for redundant badge for User - previous badges are revoked/expired

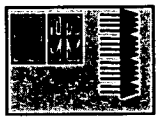


9. E-Form is auto filled at CMS from user's organizational database

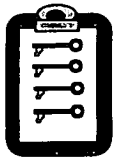


10. Badging Officer review data against credentials, signs E-Form & submits

11. CMS facility gets E-Form & validates Badging Officer signature



12. All assigned keys and certificates generated for User, wrapped in Smart Card's public key

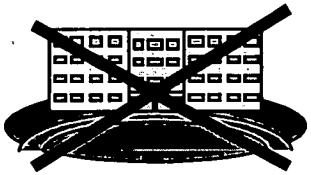


13. Badging Officer gets all assigned keys & certificates within seconds

14. Only smart card assigned to user can unwrap the private keys

15. User can update smart card automatically at own desk

16. User never visits badge office except for lost or expired badge or termination

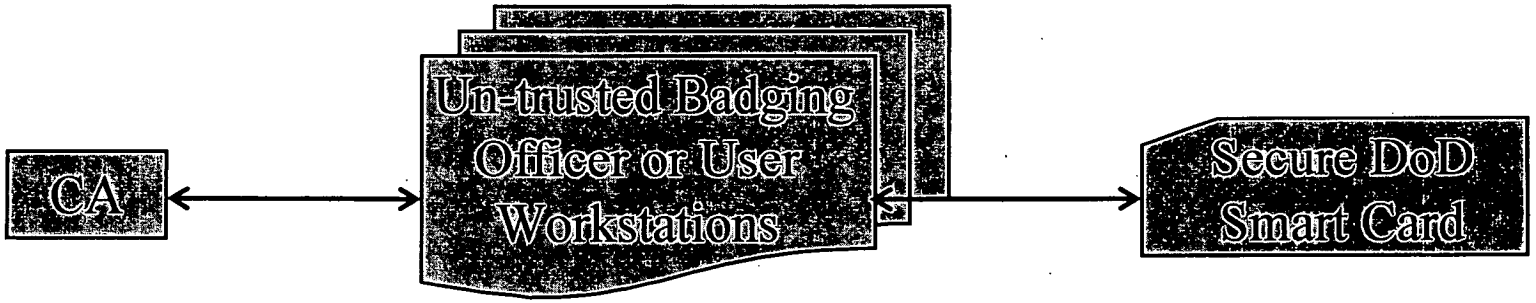


17. Badging Officer needs no trusted operating system, minimal PKI training

18. Massive reduction in operational costs with superior security

Subsequent Actions

TRW



Issuing the User's X.509 Signing Certificate:

1. Badging Officer uses un-trusted workstation to bind specific Smart Card serial number to specific user ID for that C/S/A.
2. CA wraps user's private key and signing certificate in public key of the specific Smart Card, signs the wrapped package, and sends via ***Public Key Privacy Mode*** and **Public Key Integrity Mode** of PKCS #12. Private key is marked as non-exportable. User bound to that Smart Card ID in CMS.

All subsequent Role, Group, and Encryption certificates:

1. Badging Officer not required; users can securely obtain all other certificates from any un-trusted PC or workstation.
2. CA wraps each new certificate using the user's Smart Card's public key and then signs the wrapped certificate.

Concept for Secure Forms Processing

TRW

- XML based forms from JettForms, PureEdge
- Badging Officer authenticates to RA/CA server
- Badging Officer requests badge issuance form for <User ID>, <C/S/A ID>, and <Smart Card serial number>
- CMS retrieves that C/S/A's form, assigns serial number to form, auto-fills the user's data from the authoritative database or directory, signs the form, logs it to audit trail, & issues it to Badging Officer
- Badging Officer and user validate data
- Badging Officer signs & submits finalized request

Cost / Performance Estimates

TRW

- DataCard engineers estimate that a minimum configuration DataCard 9000 can process 900 Smart Cards per hour
  - 7 parallel paths at 28 seconds per Card
  - 2 sites can process 1800 cards per hour

- ROM ~ [redacted] per 2 machines (versus [redacted])

Benefits

TRW

- Eliminates need for Badging Officers to have trusted workstations ($$)
  - Fewer points of vulnerability; lower skill levels
  - Much faster key pair generation times
- Eliminates need for 1318 remote crypto accelerators to generate key pairs ($$)
- LRA becomes simply a badging person (notary)
  - "I swear that I validated J. Doe's credentials and issued badge #130440 to him/her."
- After initial face-to-face, no need for Badging Officer for other certificate requests ($$)
- Smart Cards become integral part of central CMS
- Only CMS can load a certificate on any DoD Smart Card

Recommendations

TRW

Assess potential impacts to DoD Smart Card:

- Verify whether support for PKCS #12 is requirement under Smart Card contract(s). If so,
  - Require use of Public Key Privacy and Public Key Integrity exchange modes
  - Remove support for Password Privacy and Password Integrity exchange modes from CAC S/W
    - Note: This prevents a denial of service attack on the Smart Card.
- Assess impact of storing private key on Smart Card
- Verify whether Root CA certificate is already on CAC
- Validate potential for [redacted] cost savings

See Instructions on Website: http://webhost.tnw.com/patents/

Docket: 15-0257

Date: 2/20/01

Title of Invention: Assignment of User Certificates in Token-Enabled PKI System

Inventor(S) [See instructions on Website for assistance in determining inventorship]

(Note: to add more inventors, please press the TAB key after the last entry in the last column to insert a new row.)

Full Name **(No Initials)**	Badge	Division	CCC	TRW Mail Station	Extension	Immediate Supervisor
Kenneth Wagner Aull	150135	IS	3KLB	FP1/4165	3-5020	Bob Lentz
Thomas Carroll Kerr	130440	IS	3KLC	FP1/4165	3-5618	Kathy McLernon

*Type (NMI) if you have no middle name. Please note if you are a consultant.

Home Address	City	State	Zip Code	Home Phone	Social Security Number
Ken Aull, 5364 Lake Normandy Ct	Fairfax	VA	22030	[redacted]	[redacted]
Tom Kerr, 5348 Black Oak Dr	Fairfax	VA	22032	[redacted]	[redacted]

(No P.O. Boxes)

Conception of Invention

Date of First Written Description of the Invention: [redacted]

Identify the Written Description and Indicate Where Located:

"Card Generation Schemes.ppt" located in FP1/4165N

Date of the First Oral Disclosure: [redacted] To Whom: [redacted]

Date of First Drawings: [redacted] Present Location: FP1/4165N

Date of First Sketches: _____ Present Location: _____

Date of Formal Drawings, if any: _____ Present Location: _____

Construction And Test (Check Yes or No--double click on box you want checked.)

Invention Simulated? Yes ☐ No ☒ Date: _____ By Whom: _____

Invention Modeled? Yes ☐ No ☒ Date: _____ By Whom: _____

Invention Physically Constructed? Yes ☐ No ☒ Date: _____

Invention being implemented under existing By Whom: Ken Aull

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood by:		Witness:	Date:	Supervisor:	Date:

TRW IR&D project

Invention Successfully Tested? Yes [redacted] No [redacted] Date: [redacted]

By Whom:

Use Or Offer For Sale (Must be Completed)

Was Invention the Subject of Commercial Activity? Yes ☒ No ☐ By Whom: Ken Aull

(Commercial Activity Means External to TRW and Includes Activity with the Government) Date: [redacted]

If Yes (A) Date of First Executed Sales Contract: [redacted]

(B) Identify First Sales Contract No.: [redacted]

(C) Date Of First Delivery To Customer: [redacted]

Was Invention Described in a Proposal? Yes [redacted] No [redacted] Date: [redacted]

Was a Description of the Invention Provided to the Government? Yes [redacted] No [redacted] Date: [redacted]

Was a Description of the Invention Provided to a Commercial Customer? Yes [redacted] No [redacted] Date: [redacted]

Was a Description of the Invention Provided as Part of an On-going Contract? Yes [redacted] No [redacted] Date: [redacted]

If you answered YES to any of the above questions, please provide a copy of the material which included the description.

Is it anticipated that an activity will occur soon? Please provide the appropriate information above and enter expected date. Yes [redacted] No [redacted] Expected Date: [redacted]

Publication [Publication means printed and distributed outside TRW] (Must be Completed)

Has a Description of the Invention Been Published? Yes ☒ No ☐

If Yes, *Provide Copy* and Identify Publication and Date: Powerpoint briefing titled "Improving Key Generation & Delivery Processes for DoD Smart Cards" [redacted]

If The Invention Has Been Described in a Customer Report, *Provide Copy* and Identify the Customer Report by Customer, Date, and No.

Did the Customer Report Have a TRW Proprietary Legend? Yes [redacted] No [redacted]

Has the Invention Been Described to People Not Employed by TRW? Yes [redacted] No [redacted]

If Yes (A) Was Disclosure Under a Confidential Disclosure Agreement? Yes

(B) Provide Names of Person(S), Their Employers(S), Date, and Place of Disclosure:

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood by:		Witness:	Date:	Supervisor:	Date:

[redacted]

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood by:		Witness:	Date:	Supervisor:	Date:

Related Printed Publications and Reference Material (Must be Completed)

Identify Any Patents, Printed Publications, Written Reports, or Proposals That You Are Aware Of Relating to Closely Analogous Concepts, and *Provide Copies:*

Identify Any Prior TRW Invention Disclosures, Patent Applications, or Issued Patents Relating to the Invention:

[redacted]

Ken Aull:

Contract or Project Information (Must be Completed)

The Invention First Conceived While Charging Time to Job No.: 99X637

And Working On: DoD PKI Marketing (OITE)

☐ Government Contract or Subcontract No.: _____ Title: _____

☐ TRW Funded (IR&D, B&P, PM&P) Project No.: _____ Title: _____

☐ Commercial Contract No.: _____ Customer: _____

☒ Other, Explanation: Working as TRW Technical Fellow

Contract Administrator and Phone No.: Bob Lentz, 703-803-4904

The Invention First Constructed While Charging Time to Job No.: _____

And Working On:

☐ Government Contract or Subcontract No.: _____ Title: _____

☐ TRW Funded (IR&D, B&P, PM&P) Project No.: _____ Title: _____

☐ Commercial Contract No.: _____ Customer: _____

☐ Other, Explanation: _____

Contract Administrator and Phone No.: _____

Tom Kerr:

Contract or Project Information (Must be Completed)

The Invention First Conceived While Charging Time to Job No.: 99X637

And Working On: DoD PKI Marketing (OITE)

☐ Government Contract or Subcontract No.: _____ Title: _____

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood by:		Witness:	Date:	Supervisor:	Date:

☐ TRW Funded (IR&D, B&P, PM&P) Project No.: _____ Title: _____

☐ Commercial Contract No.: _____ Customer: _____

☒ Other, Explanation: TEDS, an Internal TRW Project sponsored by Cleveland

Contract Administrator and Phone No.: [redacted]

The Invention First Constructed While Charging Time to Job No.: _____

And Working On:

☐ Government Contract or Subcontract No.: _____ Title: _____

☐ TRW Funded (IR&D, B&P, PM&P) Project No.: _____ Title: _____

☐ Commercial Contract No.: _____ Customer: _____

☐ Other, Explanation: _____

Contract Administrator and Phone No.: _____

Tell Us All About Your Invention:

What was the problem or need that you were trying to solve?

In a conventional PKI implementation, a user who wishes to receive future certificates after receiving an initial signing certificate must return to the Tokenizing Office. If any future certificate was created in the user's environment, it would be easily compromised in transmission or via trojan horse. This required user intervention by a tokenizing office causes an increase in workload for the Tokenizing Office, requires extra training in PKI in any tokenizing office, and subjects the user's future certificates to potential compromise. The problem is to find a way for users to get an future certificate while eliminating the labor and security risk associated with assignment of these certificates by the Tokenizing office.

Inventive Concept – What is new, what it does and how it does it?

The innovative concept is allowing users to access the Certificate Management System directly in order to obtain future certificates. This is accomplished by using the information about the user in the enterprise Directory/database, along with their signing certificate, to authenticate their identity. The process will generate the user's future certificate within the CMS, and encrypt it using the user's token public key, and sign it by the CMS itself. Then it will transmit the encrypted encryption certificate to the user to be decrypted and stored on the token.

Since the key pair is generated at the CMS, it is done at the highest security. Since the key and certificate are wrapped by the public key of the token assigned to a user, the key cannot be compromised by the transmission system or the user's workstation. Only the token assigned to the

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood by:		Witness:	Date:	Supervisor:	Date:

user can "activate" these future certificates and private keys. Because of this, the user workstation does not need to be secure or trusted

Invention Description and Operation: (Attach Drawings Or Sketches for Each Embodiment)

First a User inserts a token into a workstation's token reader and loads Certificate Management System web page. The CMS web page locates the signing certificate on token, validates User. Then, the Certificate Authority authenticates user's signing certificate and token serial number. The CA generates User's new required keys and corresponding certificates, which it wraps (encrypts) using the token's public key. The package is signed by the CMS system. The User downloads the encrypted certificate/key as a high security encrypted and signed package. Finally, the User loads the high security data package onto their token and only the token can decrypt the certificates and keys for use by the User.

Briefly describe what the prior art taught:

[redacted]

What are the <u>advantages</u> to your invention?

This invention allows the user to obtain future certificate/key directly from the certificate management system, without compromising high security. This eliminates the need for return visits to the Tokenizing office, reducing Tokenizing workload and increasing the integrity of the assigned future certificates and private keys. Full security is maintained, since the future certificate/key can only be "activated" on the token known to have been assigned to the user.

Government, Industrial or commercial applications:

What are the current plans, if any, for the concepts discussed in the Invention Disclosure? If none, please so state.

[redacted]

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood by:		Witness:	Date:	Supervisor:	Date:

Is there an intended TRW commercial product that will use the concepts in this Invention Disclosure?

There is a "product" in the sense that S&ITG will offer at a pre-defined price with a pre-defined schedule a PKI "solution" to both commercial and government customers. That product is still being defined. Multiple divisions are participating in the definition of the product.

If Yes, what is the intended commercial product?

The product is an "e-business" solution that provides digital signatures and paperless workflow to an enterprise.

If Yes, when will the intended commercial product be developed?

Is there an intended TRW generic use for the concepts in this Invention Disclosure?

If Yes, what is the intended generic use?

(Obtain All Signatures Before Sending to Patent Counsel)

Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Inventor:	Date:	Inventor:	Date:	Inventor:	Date:
Witnessed, Read and Understood by:		Witness:	Date:	Supervisor:	Date:

Supplemental One Sheet Description - In Viewgraph Format, Tell Us About Your Invention (To be Used at Invention Evaluation Committee Meeting)

Title: Assignment of User Certificates in Token-Enabled PKI System

Summary of Idea:

The process of assigning role and encryption certificate/keys to a user by utilizing previously affirmed information about the user, using only a token-enabled workstation available to the user.

What Do You Believe is the Innovative Concept:

The process of assigning role and encryption certificate/keys to a user without the need for a human intermediary. The primary identity certificate/key downloaded to a token allows the *bound together* holder of the token to request any and all future PKI certificates. Once the user has been bound to a token, and the primary identity certificate on the same token has been asserted, it is safe to create and download any and all future certificates and keys. The process of using the PKI Certificate Management System to assign a certificate and a private key to a user is critical. The CMS encrypts and signs the certificate and private key for transmission to the user in such a way that only the user's token will be able to validate, decrypt and activate the certificate and private key (via PKCS12 encryption using the Primary Token Identity Certificate). Since the token and the user are permanently bound together, the CMS system may safely wrap in the public key of the token all keys and certificates which are destined for a particular user.

What is the Closest Prior Art Known to You:

[redacted]

List Competitive Advantages:

[redacted]

Reason Why We Should File a Patent for Your Invention:

Concept is potentially profitable for TRW, particularly as we pursue PKI-related contracts.

TRW Inc.

One Space Park
Redondo Beach, CA 90278
310.812.4321
E2/6051
310.812.1534
Telecopier 310.812.2687
E-mail: lorna.schott@trw.com

Law Department

DES

Call up draft [redacted]
Call up App [redacted]

April 27, 2001

VIA TELECOPIER

Donald E. Stout, Esq.
Antonelli, Terry, Stout & Kraus, LLP
Suite 1800
1300 North Seventeenth Street
Arlington, Virginia 22209

199 40032X00
1st draft due [redacted]

Subject: TRW Docket No. 15-0257
Last Day to File Application: [redacted]
Gov't. Contract No.: **NGC**
Billing Unit: SITG/IS - Billing Code: 312

Dear Don:

[redacted]

Faxed herewith is a copy of the above-referenced invention disclosure. No formal patentability search will be conducted in this matter. This may be related to TRW Docket Nos. [redacted], [redacted], and [redacted]. Please review these cases to see if they are related, and if so, should they be filed on the same day.

The first draft application should be submitted to this office by [redacted] Please follow the new format for preparing the patent application based on the new Rules and Regulations (see Federal Register/Vol. 65, No. 175/Friday, 9/8/00). The draft application and drawings should be sent by regular U.S. mail, along with a soft copy on disk. It is also possible to send the draft application via PgP Encryption. Please obtain approval from this office before submitting it PgP.

You should also be aware that all transmittals of drafts and comments should be directed to this office, and not directly between you and the inventor, so that I can keep track of the progress of the preparation. If you need to deviate from any of the above procedures, please contact me immediately.

Attached is a list of standards that we are now requiring for all patent application preparation. Please follow these guidelines.

The transmittal should indicate whether or not there are any statutory bars running of which you are aware, and whether or not there are any impediments to our filing corresponding foreign applications. **Your firm is also responsible for informing us if there are any related and/or co-pending applications that are to be filed at the same time.**

So that there is no question as to division of responsibilities, this office will be responsible for the preparation of the formal papers (declaration, power of attorney, assignment) and the actual filing of the application.

I look forward to working with you to obtain the best patent coverage we can for this invention. If you have any questions concerning this case, please do not hesitate to contact me.

Sincerely,

Lorna L. Schott
Patent Administrator

/lls
Enclosure

PATENT APPLICATION PREPARATION STANDARDS

- The first page of the application should include: Title, Headings for Cross-reference and/or Government clauses, only when applicable (leave out if not applicable), followed by Background, Summary of Invention, etc. Do not include a separate Cover/Title page,
- The header should contain the TRW Docket Number in the upper right hand corner, as well as the Express Mail, mailing language,
- Standard government contract clause inserted upon first draft, when applicable,
- Specification with claims,
- Drawings prepared in semi-formal format (no shading – see Guide for the Preparation of Patent Drawings – Dept. of Commerce),
- Information Disclosure Statement and Form PTO-1449 signed by you,
- Abstract (no longer than 150 words, not including the title) with reference numerals suitable for filing in foreign jurisdictions,
- Title of patent application on the abstract,
- Draft application on 8 ½" x 11" bond paper (Please follow the new format as stated in the Rules and Regulations – Federal Register/Vol. 65, No. 175),
- Copy of the application (initial drafts and subsequent drafts) on diskette readable by Microsoft Word running on a P.C. enclosed in a protective cover.
- The transmittal should also indicate whether or not there are: any related cases, statutory bars running of which you are aware, and whether or not there are any impediments to our filing corresponding foreign applications.
- **You may conduct your interview directly with the inventors. Make sure that all correspondence and documents exchanged between you and the inventors are forwarded to this office.**

DONALD R. ANTONELLI
DAVID T. TERRY
MELVIN KRAUS
WILLIAM I. SOLOMON*
GREGORY E. MONTONE
RONALD J. SHORE
DONALD E. STOUT
ALAN E. SCHIAVELLI
JAMES N. DRESSER
CARL I. BRUNDIDGE*
PAUL J. SKWIERAWSKI*
ROBERT M. BAUER

RANDALL S. SVIHLA
HUNG H. BUI*
GEORGE N. STEVENS*
FREDERICK D. BAILEY
DAVID C. OREN
RALPH T. WEBB*

*ADMITTED OTHER THAN VA

LAW OFFICES
ANTONELLI, TERRY, STOUT & KRAUS, LLP
SUITE 1800
1300 NORTH SEVENTEENTH STREET
ARLINGTON, VIRGINIA 22209

OF COUNSEL
HENRY M. ZYKORIE*
ROBERT F. GNUSE

PATENT AGENT
LARRY N. ANAGNOS

TELEPHONE
(703) 312-6600
FACSIMILE
(703) 312-6666

EMAIL
email@antonelli.com

June 25, 2001

Ms. Lorna L. Schott
Patent Administrator
Law Department
TRW Inc.
One Space Park
Redondo Beach, California 90278

Re: New U.S. Application
TRW Docket No. 15-0257
"Assignment of User Certificates in Token Enabled Public Key Infrastructure System"
Inventors: Kenneth Aull and Thomas Kerr
ATS&K Ref: 199.40032X00

Dear Lorna:

Further to your letter of April 27, 2001, please find enclosed the draft application referenced above. This package includes the draft application, IDS, 1449 form, reference, declaration and assignment as well as electronic copies of these documents. TRW Docket Numbers 15-0254, 15-0255 and 15-0256 will be arriving separately.

It should be noted that TRW Docket Numbers 15-0254, 15-0255, 15-0256, and 15-0257 a[redacted]should all be filed on the same day in the U.S. Patent and Trademark Office.

Should you have any questions please do not hesitate to contact us. Please note that the Federal Express charges are being absorbed by our firm.

Very truly yours,
Antonelli, Terry, Stout & Kraus, LLP

George N. Stevens

TRW Inc.

One Space Park
Redondo Beach, CA 90278
310.812.4321
Direct Dial No. 310.812.1534
Telecopier 310.812.2687
Building E2/6051

Law Department

GNS

199.40032X00
REVISED APPLN 11/1/01
DES

October 18, 2001

George N. Stevens, Esq.
Antonelli, Terry, Stout & Kraus, LLP
1300 North Seventeenth Street, Ste. 1800
Arlington, VA 22209

Subject: TRW Docket No. 15-0257; Your File No. 199.40032X00
Title: ASSIGNMENT OF USER CERTIFICATES IN TOKEN ENABLED PUBLIC KEY INFRASTRUCTURE SYSTEM

Dear George:

Enclosed please find the inventor's first review comments in connection with the above-referenced application. TRW will prepare the formal drawings. [redacted] Please incorporate these changes and return the revised application to me **no later than November 1, 2001** and include an electronic version on disk in Word 6.0 for the PC.

For your convenience, I have also enclosed the disk submitted with the original draft application.

Thank you for your attention in this matter.

Sincerely,

Lorna mlb

Lorna L. Schott
Patent Administrator

/mlb

Enclosures

DONALD R. ANTONELLI
MELVIN KRAUS
WILLIAM I. SOLOMON*
GREGORY E. MONTONE
RONALD J. SHORE
DONALD E. STOUT
ALAN E. SCHIAVELLI
JAMES N. DRESSER
CARL I. BRUNDIDGE*
PAUL J. SKWIERAWSKI*
ROBERT M. BAUER

RANDALL S. SVIHLA
HUNG H. BUI*
GEORGE N. STEVENS*
FREDERICK D. BAILEY
DAVID C. OREN
RALPH T. WEBB*

*ADMITTED OTHER THAN VA

LAW OFFICES
ANTONELLI, TERRY, STOUT & KRAUS, LLP
SUITE 1800
1300 NORTH SEVENTEENTH STREET
ARLINGTON, VIRGINIA 22209

OF COUNSEL
DAVID T. TERRY
HENRY M. ZYKORIE*
ROBERT F. GNUSE
HAROLD A. WILLIAMSON*

PATENT AGENT
LARRY N. ANAGNOS

TELEPHONE
(703) 312-6600
FACSIMILE
(703) 312-6666

EMAIL
email@antonelli.com

October 24, 2001

Ms. Lorna L. Schott
Patent Administrator
Law Department
TRW Inc.
One Space Park
Redondo Beach, California 90278

Re: AULL et al.
Title: "Assignment of User Certificates in Token Enabled Public Key Infrastructure System"
Our Ref: 199.40032X00 - Your Ref.: 15-0257

Dear Lorna:

In response to your letter of October 18, 2001, please find enclosed a paper copy and soft copy of the revised patent application referenced above. It should be noted that we have not precisely followed the changes requested by the inventors. Specifically, we have placed the insert requested into paragraphs 11, 12, 27, 28, and 32.

It is our understanding that TRW will be supplying the revisions to Fig. 1. Please have the inventors further review the enclosed application.

Thank you for entrusting the preparation of this application to us. Should you have any questions, please do not hesitate to contact the undersigned attorney.

Very truly yours,

George N. Stevens
Antonelli, Terry, Stout & Kraus, LLP

GNS/pay

Enclosures